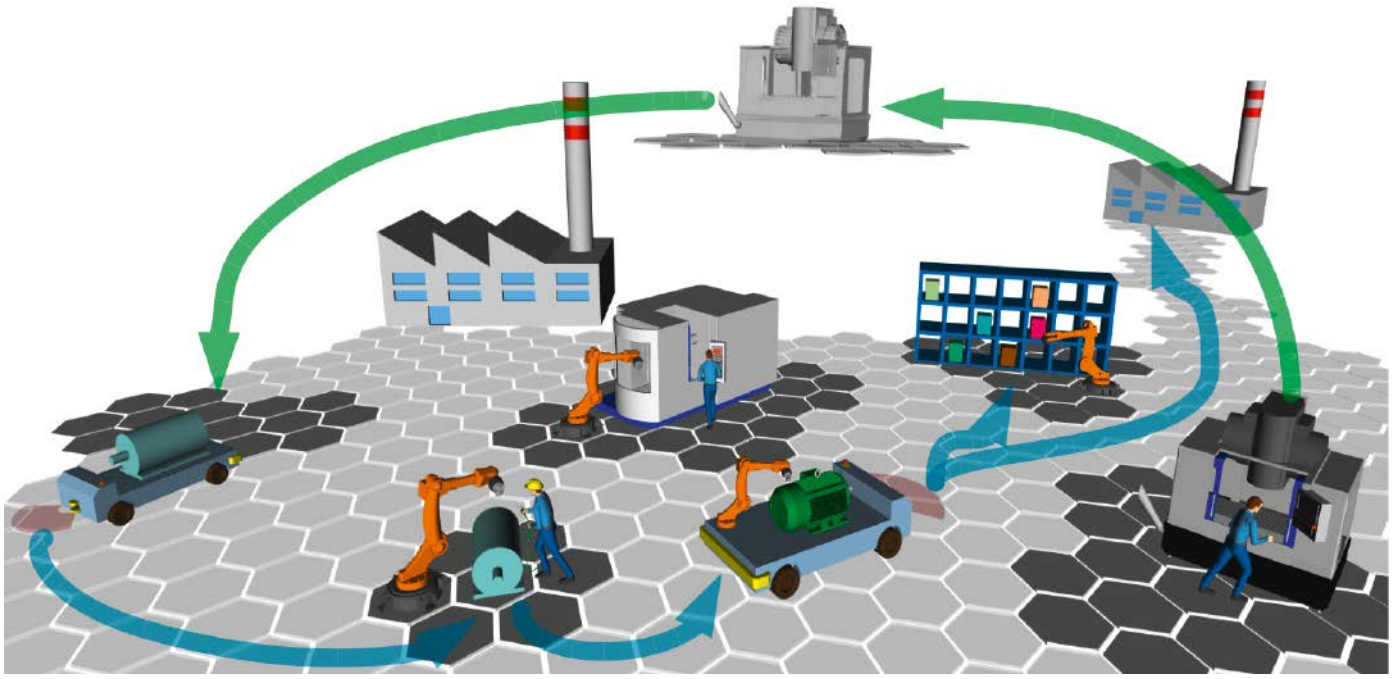

BJÖRN KASPER · STEFAN VOSS

Neue Anforderungen an die Sicherheitsnachweisführung von Maschinen und Anlagen im Kontext von Industrie 4.0

Auch bei Industrie 4.0-Anwendungsszenarien ist die Sicherheit der Beschäftigten zu gewährleisten. Dazu müssen auf Grund des hohen Vernetzungsgrades neben den bisher berücksichtigten sicherheitstechnischen Aspekten der funktionalen Sicherheit in verstärktem Maße die industrielle Angriffssicherheit (Security) sowie deren Wechselwirkungen untereinander betrachtet werden. Aus Sicht des Arbeitsschutzes sind insbesondere Security-Aspekte mit Auswirkungen auf die funktionale Sicherheit zu betrachten.

1. Selbstorganisierende Produktionssysteme der Industrie 4.0

Der Begriff „Industrie 4.0“ steht für die vierte industrielle Revolution. Basierend auf der rasant zunehmenden Digitalisierung von Wirtschaft und Gesellschaft und der Verschmelzung der industriellen Produktion und Fertigung mit modernster Informations- und Kommunikationstechnik (IKT) wird eine intelligente Organisation und Steuerung der Wertschöpfungskette über alle Phasen des Lebenszyklusses eines Produktes möglich. Dadurch lassen sich Kundenwünsche von der Produktidee bis hin zum Recycling, einschließlich der damit verbundenen Dienstleistungen, mitdenken. Darüber hinaus könnten leichter als bisher maßgeschneiderte Produkte nach individuellen Kundenwünschen produziert werden [vgl. 4]. Nach der Dampfmaschine (1. Industrielle Revolution), dem Fließband (2. Industrielle Revolution), der Elektronik und der Informationstechnik (3. Industrielle Revolution) bestimmen nun intelligente Fabriken (sogenannte „Smart Factories“) die Entwicklung [vgl. 4].

Wesentliche technische Grundlagen der Industrie 4.0 sind intelligente, digital vernetzte Systeme, sog. cyber-physische Systeme (CPS). Mit ihrer Hilfe soll eine weitestgehend selbstorganisierte Produktion möglich werden: Menschen, Maschi-

nen, Anlagen, Logistik und Produkte kommunizieren und kooperieren in der Industrie 4.0 direkt miteinander. Produktions- und Logistikprozesse zwischen Unternehmen im selben Produktionsprozess können intelligent miteinander verzahnt werden, um die Produktion effizienter und flexibler zu gestalten [vgl. 4].

2. Sicherheitstechnische Aspekte von Maschinen und Anlagen

Jede Maschine oder Anlage besitzt *Betriebsfunktionen*, die zur eigentlichen Wertschöpfung beitragen. Mögliche Gefährdungen und Risiken werden durch entsprechende Sicherheitsmaßnahmen minimiert. Neben den klassischen Sicherheitsmaßnahmen wie z. B. festen, trennenden Schutzeinrichtungen werden Maßnahmen der funktionalen Sicherheit eingesetzt. Solche *Sicherheitsfunktionen* bestehen stets aus sicherheitsgerichteten Sensoren (bspw. Lichtgitter, Laserscanner), der sicherheitsgerichteten Logik (Sicherheitsprogramm auf der Maschinensteuerung) sowie der sicherheitsgerichteten Aktorik (schnelles Stillsetzen des Hauptantriebes mit definierten und überwachten Bremsrampen). Damit wird gewährleistet, dass Fehlerzustände im Bearbeitungsprozess erkannt werden können und die vorgesehene Schutzwirkung eintritt.

Für alle sicherheitstechnischen Betrachtungen ist entscheidend, zwischen den *Betriebs- und Sicherheitsfunktionen* einer Maschine zu unterscheiden. Sicherheitsfunktionen zur Erreichung der funktionalen Sicherheit werden oft als *Safety-Funktionen* bezeichnet. Die sicherheitsgerichtete Logik wertet hierbei die Signale der Sensorik (z. B. Lichtgitter) aus und veranlasst im Ernstfall den Aktor (Maschinenantrieb), in einen sicheren Zustand (Stillstand) zu gehen. Wenn diese sicherheitsgerichteten Signale über weite Strecken oder besonders im Kontext der Industrie 4.0-Konzepte über ungesicherte Medien (z. B. funkbasierte Netzwerke) übertragen werden, müssen geeignete *Security-Maßnahmen* zur Manipulationsvermeidung ergriffen werden. Entsprechende Security-Maßnahmen sind z. B. die Verschlüsselung der Kommunikation oder die gezielte Reduktion von Funk-Reichweiten.

3. Die Sicherheitstechnik der Industrie 4.0

Um auch im Kontext zukünftig denkbarer Industrie 4.0-Anwendungsszenarien Sicherheit und Gesundheitsschutz der Beschäftigten zu gewährleisten, sind bei der Umsetzung der Konzepte von Industrie 4.0 neue Herausforderungen bezogen auf die sichere Gestaltung von Maschinen- und Anlagenteilen und weiterer Komponenten sowie der Prozessabläufe zu bewältigen.

Wie im vorigen Abschnitt dargestellt, folgt der bisherige Stand der Sicherheitstechnik dem deterministischen Sensor-Logik-Aktor-Prinzip. Es steht allerdings zu erwarten, dass in der stärksten Ausprägung von Industrie 4.0 Algorithmen aus dem Bereich des Maschinellen Lernens zukünftig auch im Maschinen- und Anlagenbau Verwendung finden werden, um die Produktionsprozesse flexibel und intelligent miteinander zu verknüpfen [vgl. 7].

Darüber hinaus ist denkbar, dass auch Signale aus sicherheitsgerichteten Funktionen und Steuerungen in diese Entwicklung einbezogen werden könnten. Die sicherheitsgerichtete Reaktion ergibt sich dann nicht mehr deterministisch aufgrund zuvor definierter und reproduzierbarer Zustände, sondern auf der Grundlage einer *Wahrscheinlichkeitsanalyse* zur Laufzeit. Dazu müssen die verwendeten Signale und Daten noch nicht einmal wie bisher zwingend aus sicherheitsgerichteten Quellen stammen. Die Zuverlässigkeit könnte durch algorithmische Plausibilitäten, d. h. einem Abgleich mit anderen Signalen und Daten sichergestellt werden. Damit wird die Sicherheit einer Maschine zukünftig primär von der Sicherheit und Zuverlässigkeit lernfähiger Software-Algorithmen abhängen. Neben vielen sich dadurch ergebenden Herausforderungen (insbesondere in Bezug auf die Sicherheitsnachweisführung) besteht auch die Chance, durch Auswertung der vorhandenen Datenmenge zurückliegender Ereignisse und Situationen mithilfe stochastischer Methoden des maschinellen Lernens, in jedem Moment potenziell gefährliche Situationen „vorhersehen“ zu können [vgl. 7].

4. Neue Anforderungen an sicherheitstechnische Analyse- und Bewertungs-Methoden

Hinsichtlich der Sicherheit heutiger Maschinen und Anlagen und besonders im Kontext der Industrie 4.0 sind zwei Aspekte zu berücksichtigen: Zum einen die Produkt- und Betriebssicherheit (engl. *Safety*) sowie zum anderen die Angriffs- und Manipulationssicherheit der verwendeten Informations- und Netzwerk-Technologie (engl. *Security*). Beide Aspekte können sich gegenseitig beeinflussen. Aus Sicht des Arbeitsschutzes gilt es, diese Zusammenhänge zu betrachten. So kann mangelhafte Angriffssicherheit durch Manipulation der Maschinensteuerung(en) beispielsweise über deren Vernetzungen untereinander zum Ausfall von Schutzfunktionen führen und damit zur Gefahr für die Beschäftigten werden. Diese beiden Sicherheits-Aspekte werden bislang methodisch einzeln betrachtet, indem Risikobeurteilungen getrennt für die Aspekte Safety und Security durchgeführt werden. In Abb. 1 ist schematisch eine Maschine mit ihren Betriebs- und Sicherheitsfunktionen in Form eines Prozessschaubildes dargestellt. Die darauf wirkenden Aspekte der Maschinensicherheit sowie

DIE AUTOREN

Björn Kasper
Wissenschaftlicher Mitarbeiter der Gruppe Arbeitsstätten, Maschinen- und Betriebssicherheit, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dresden; Bearbeitung der Themenfelder Industrie 4.0, funktionale Maschinen- und Anlagensicherheit sowie netzwerktechnische Angriffssicherheit
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dresden
BAuA-Informationszentrum:
info-zentrum@baua.bund.de

Dr. Stefan Voß
Leiter der Gruppe Arbeitsstätten, Maschinen- und Betriebssicherheit, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dresden

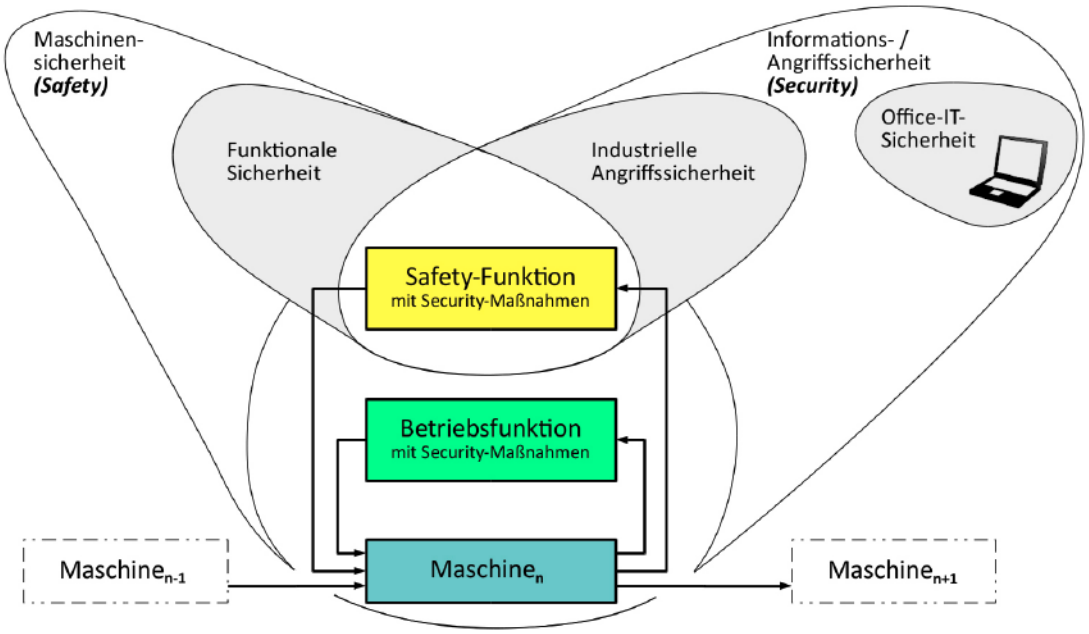

Abb. 1: *Betriebs- und Sicherheitsfunktionen von Maschinen und Anlagen [angelehnt an 6]*

der Informations- und Angriffssicherheit, die den Bereich der Office-IT-Sicherheit mit einschließt, wurden als Schnitt- und Teilmengen in Form eines Venn-Diagrammes eingezeichnet.

In heutigen Produktionsanlagen werden marktbedingte Absatz- und Variantenschwankungen meist mit einem *Ressourcenvorhalt* berücksichtigt. Die damit erreichbare *Flexibilität* einer Anlage umfasst die Änderungsmöglichkeiten, die eine Anlage von sich aus mitbringt, um auf zum jeweiligen Planungszeitpunkt bekannte Änderungen reagieren zu können. Innerhalb zuvor vereinbarter Grenzen kann die flexible Anlage sehr schnell und mit geringem Aufwand auf die geänderten Randbedingungen angepasst werden [5].

Zukünftig werden deutlich dynamischere und volatilere Märkte erwartet, wodurch der dafür erforderliche Flexibilitätsvorhalt nicht mehr wirtschaftlich wäre. Aus diesem Grund werden im Kontext von Industrie 4.0 wandlungsfähige Fertigungsanlagen durch auftragsbezogene Rekombination von Fertigungsmodulen diskutiert. Die *Wandlungsfähigkeit* einer Anlage beschreibt dabei ihr Vermögen und Potenzial, mit minimalem Aufwand beliebig umgestaltet zu werden [vgl. 5]. Diese Wandlungsfähigkeit wird erreicht, indem einzelne Fertigungsmodule zu Fertigungsinseln rekombiniert, vernetzt und automatisch konfiguriert werden (siehe grüne Pfeile im Aufmacherbild[1]). Einzelmodule (sog. Industrie 4.0-Komponenten) werden dazu flexibel und zumeist funkbasiert miteinander vernetzt. Erst dadurch kann das zu fertigende Produkt seinen eigenen Herstellungsprozess steuern (blaue Pfeile). Diese automatisch ablaufenden Prozesse der Rekombination, Vernetzung und Konfiguration von Einzelmodulen zu einem dynamischen Gesamtsystem können durch Algorithmen des maschinellen Lernens unterstützt werden.

Dadurch ergeben sich zur Laufzeit der Anlage Systeme aus (Teil-)Systemen, die zu einer grundlegenden Steigerung der kombinatorischen Komplexität des Gesamtsystems führen. Damit verbunden ist ein stetig sinkendes Systemverständnis durch einzelne Experten [vgl. 2]. Die Struktur und das Gesamtverhalten sowie die Abhängigkeiten der Systemkomponenten untereinander können zur Entwicklungszeit der Einzelsysteme nicht oder nur schwer vorhergesagt werden. Bei Fehlfunktionen und Störungen einzelner Komponenten könnten leichter Kettenreaktionen eintreten, die zu wesentlich größeren negativen Konsequenzen für die Gesamtanlage führen [vgl. 2].

Diese Eigenschaften führen zu Unsicherheiten in der Aussage über das zu erwartende Gesamtsystemverhalten. Dadurch kommen die heute verfügbaren Methoden zur Analyse und Bewertung der funktionalen Sicherheit an ihre Grenzen, da solche dynamischen Systeme bzw. Szenarien von den aktuellen Sicherheitsnormen nicht erfasst werden.

Die heutigen sicherheitstechnischen Konzepte (vor allem bezüglich Safety) sowie die Methoden zur Sicherheitsnachweisführung beruhen bislang zentral auf der Annahme eines deterministischen, vorhersagbaren Systemverhaltens [vgl. 3]. Von diesem deterministischen Verhalten konnte bisher ausgegangen werden, wenn in der Kons-

[1] Bild angelehnt an Smart Micro Factory, Fraunhofer IML.

truktions- und Designphase definierte Anlagen zugrunde gelegt werden, in denen zwar variable aber vorab klar definierte Prozesse ablaufen. Die sicherheitstechnischen Standards gehen heute davon aus, dass ein System vor seiner sicherheitstechnischen Abnahme und Zulassung vollständig entwickelt und konfiguriert ist [vgl. insbes. 1]. Danach dürfen keine sicherheitsrelevanten Veränderungen (auch Reparaturen) vorgenommen werden, ohne dass eine erneute sicherheitstechnische Überprüfung und Abnahme zumindest der betroffenen Teilsysteme erfolgt.

Damit sind die in der Fachwelt diskutierten Industrie 4.0-Anwendungsszenarien mit den heutigen Methoden zur Analyse und Bewertung der funktionalen Sicherheit nicht oder nur mit erheblichen Einschränkungen hinsichtlich der zur Laufzeit zulässigen Dynamik, Variabilität, Wandelbarkeit und Lernfähigkeit der Maschinen bzw. der verfahrenstechnischen Anlagen validierbar. Daher ergibt sich der Bedarf, die heutigen sicherheitstechnischen Methoden an die neuen bzw. geänderten Anforderungen wandlungsfähiger Fertigungsanlagen anzupassen oder weiterzuentwickeln.

5. Industrie 4.0-Anwendungsszenarien und Bewertung ihrer sicherheitstechnischen Aspekte

Zur Beurteilung des aktuellen Standes der Technologieentwicklung im Kontext von Industrie 4.0 wurde durch die BAuA eine Literaturstudie erarbeitet. Dabei war der Fokus, einen Überblick über wesentliche Grundlagen und Zusammenhänge von Industrie 4.0-Konzepten sowie ausgewählte Anwendungsszenarien zu erhalten. Die untersuchten Anwendungsszenarien betrachteten jeweils verschiedene Facetten der Industrie 4.0-Konzepte mit unterschiedlichen Wichtungen. Keines der Anwendungsszenarien beleuchtete alle Aspekte der Industrie 4.0-Konzepte in gleichem Maße.

Um die Sicherheit der Beschäftigten zu gewährleisten, müssen bei Anwendungsszenarien im Kontext von Industrie 4.0 durch den hohen Grad der Vernetzung dezentraler Teilsysteme mit Hilfe von IKT neben den bisher vorwiegend berücksichtigten sicherheitstechnischen Aspekten der funktionalen Sicherheit (Safety) in verstärktem Maße die industrielle Angriffssicherheit (Security) sowie deren Wechselwirkungen untereinander betrachtet bzw. berücksichtigt werden. Bei der sicherheitstechnischen Bewertung der ausgewerteten Anwendungsszenarien hat sich gezeigt, dass nur einige der in der Literatur beschriebenen Anwendungsszenarien die Aspekte der funktionalen Sicherheit betrachtet haben. Jedoch adressierte keines der untersuchten Anwendungsszenarien inhaltlich die industrielle Angriffssicherheit. Demzufolge wird auch in keinem der betrachteten Anwendungsszenarien ein Zusammenhang zwischen funktionaler Sicherheit (Safety) und industrieller Angriffssicherheit (Security) hergestellt bzw. mögliche Wechselwirkungen zwischen beiden Sicherheitsaspekten dargestellt oder näher untersucht. Es werden in den zur Verfügung stehenden Literaturquellen der betrachteten Anwendungsszenarien keine Risikoanalysen und -bewertungen durchgeführt oder Maßnahmen zur Risikominderung aufgezeigt.

6. Ausblick

Zusammenfassend ist festzustellen, dass die sicherheitstechnische Bewertung von Industrie 4.0-Prozessen und -Systemen eine Reihe offener Fragestellungen aufwirft und aufgrund der facettenreichen Aspekte eine hohe Interdisziplinarität vorliegt. Dabei stehen u. a. Fragen im Raum, inwieweit die Sicherheit von Maschinen und Anlagen im Kontext von Industrie 4.0 aufgrund ihrer Wandlungsfähigkeit oder sogar Lernfähigkeit ihrer Betriebsfunktionen gewährleistet werden kann. Insbesondere sollte zukünftig untersucht werden, wie die Wechselwirkungen von funktionaler Sicherheit und industrieller Angriffssicherheit zu bewerten sind bzw. ob diese über heute verfügbare sicherheitstechnische Bewertungsmethoden erfasst werden und identifizierte Risiken mit angemessenen Maßnahmen reduziert werden können. ■

LITERATUR

[1] DIN EN 61508-3:2011-02, VDE 0803-3:2011-02. Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010).

[2] Leopold, Helmut. 2015. Sicherheit im elektronischen Universum: Neue Bedrohungspotenziale brauchen effektive Gegenstrategien und eine gemeinsame gesellschaftliche Anstrengung.

[3] Liggesmeyer, Peter und Mario Trapp. 2016. Safety in der Industrie 4.0: Herausforderungen und Lösungsansätze. In: Handbuch Industrie 4.0 Bd.1: Produktion, 107–123. Springer-Verlag GmbH.

[4] Plattform Industrie 4.0. 2017. Was ist Industrie 4.0? Die vierte industrielle Revolution: Auf dem Weg zur intelligenten und flexiblen Produktion.

[5] Steegmüller, Dieter und Michael Zürn. 2016. Wandlungsfähige Produktionssysteme für den Automobilbau der Zukunft. In: Handbuch Industrie 4.0 Bd. 1: Produktion, 27–44. Springer-Verlag GmbH.

[6] VDE-AR-E 2802-10-1:2017-04. Zusammenhang zwischen funktionaler Sicherheit und Informationssicherheit am Beispiel der Industrieautomation – Teil 1: Grundlagen.

[7] Wickert, Karl. 2017. Algorithmen: Chance und Herausforderung für die Maschinensicherheit. sicher ist sicher, Nr. 12/2017: 531–533.